

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Seiji HIGURASHI

Serial No.

Filed: October 27, 2000

For: METHOD AND APPARATUS
FOR TRANSMITTING
ENCRYPTION-RESULTANT
INFORMATION AND
DECRYPTING
INFORMATION

Art Unit:

Examiner:

Atty Docket: 0102/0141

SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Attached hereto please find a certified copy of applicant's Japanese application No. 11-335502 filed in Japan on November 26, 1999. Applicant requests the benefit of said November 26, 1999 filing date for priority purposes pursuant to the provisions of 35 USC 119.

Respectfully submitted,



Louis Woo, Reg. No. 31,730
Law Offices of Louis Woo
1901 N. Fort Myer Drive, Suite 501
Arlington, Virginia 22209
Phone: (703) 522-8872

Date:

Oct 27 2000

#2
10813 U.S. PTO

09/697084

10/27/00

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENTJCE13 U.S. PTO
09/697084

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年11月26日

出 願 番 号
Application Number:

平成11年特許願第335502号

出 願 人
Applicant(s):

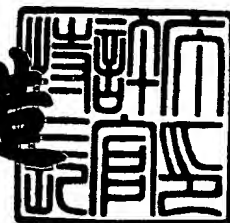
日本ビクター株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 9月22日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3076191

【書類名】 特許願

【整理番号】 411001518

【提出日】 平成11年11月26日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 G11B 20/10
G11B 20/12
H04N 5/91

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 日暮 誠司

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【代表者】 守随 武雄

【代理人】

【識別番号】 100085235

【弁理士】

【氏名又は名称】 松浦 兼行

【手数料の表示】

【予納台帳番号】 031886

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報伝送方法、記録方法及び記録媒体

【特許請求の範囲】

【請求項 1】 暗号化した所望の情報と、この所望の情報を誤り訂正する誤り訂正符号とを、再生側で正規のユーザに対してのみ暗号を解除して再生可能とするための、暗号解除情報と共に伝送する情報伝送方法において、前記誤り訂正符号の完結周期内に、少なくとも一つの前記暗号解除情報を分散配置して伝送することを特徴とする情報伝送方法。

【請求項 2】 暗号化した所望の情報と、この所望の情報を誤り訂正する誤り訂正符号とを、再生側で正規のユーザに対してのみ暗号を解除して再生可能とするための、暗号解除情報と共に同じ記録媒体に記録する記録方法において、前記誤り訂正符号の完結周期内に、少なくとも一つの前記暗号解除情報を分散配置して前記記録媒体に記録することを特徴とする記録方法。

【請求項 3】 少なくとも映像情報を含む所望の情報と、この所望の情報の所定数の記録トラック又は記録セクタ周期で完結する前記所望の情報の誤り訂正符号とを暗号化して、デジタル信号形態で同じ記録媒体に記録する記録方法において、

再生側で正規のユーザに対してのみ暗号を解除して再生可能とするための暗号解除情報を、前記所定数の記録トラック又は記録セクタ周期内で分散配置して少なくとも一つ記録することを特徴とする記録方法。

【請求項 4】 前記記録媒体は磁気テープであり、前記所望の情報として映像情報を少なくとも含むデジタル信号が記録されていることを特徴とする請求項 3 記載の記録方法。

【請求項 5】 少なくとも映像情報が誤り訂正符号と共に暗号化されて固定長のデータブロック単位で予め定められたデータブロック数の各トラックに記録されているテープ状記録媒体であって、前記誤り訂正符号は複数トラックで完結するように記録されており、前記映像情報と誤り訂正符号の暗号化を正規の再生装置で解除するための暗号解除情報が、前記誤り訂正符号の完結トラックと同じトラック単位で完結するように分散配置

されていることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は情報伝送方法、記録方法及び記録媒体に係り、特に記録媒体にパケット化して記録されたデジタル情報の著作権保護のための伝送、例えば記録、再生等を行う情報伝送方法、記録を行う記録方法及び記録媒体に関する。

【0002】

【従来の技術】

映像情報や音声情報が記録されている記録済みの記録媒体を正規に購入したユーザのみに、当該記録媒体の記録情報を正常に再生させることができるようにすることにより、著作権の保護を図る技術の一つとして、記録情報を暗号化して記録すると共に、暗号解除情報を上記の暗号化された情報の記録領域とは異なる領域（例えば、リードイン領域）に記録しておく方法が、ディスク装置の分野では知られている。

【0003】

従って、このディスク装置では、正規のユーザが使用する再生装置でのみ、記録媒体であるディスクから再生された暗号解除情報に基づき、暗号化されている再生情報を復号することができる。

【0004】

【発明が解決しようとする課題】

しかるに、ディスク装置では暗号化されている情報と、暗号解除情報とが、同じディスクの異なる領域に記録されていても、ディスク装置ではランダムアクセスが可能であるので、暗号の解読は短時間で支障なく行えるが、上記の暗号化技術をVTRのような磁気テープの記録再生装置に適用した場合は、暗号解除情報のアクセスに時間がかかり、特にテープ中途からの再生に支障をきたし、実用的でない。

【0005】

また、暗号解除情報を暗号化されているコンテンツ情報と同じ領域に記録して

いた場合は、両者の同期が問題となり、どのエリアのコンテンツ情報とどの暗号解除情報とが対応するのかが分からなくなったり、メモリを余分に必要としたり、デコードするまでに時間がかかるといった問題が生じる。

【0 0 0 6】

本発明は以上の点に鑑みなされたもので、テープ状記録媒体に対しても、実用上支障なく、暗号化された情報の再生が可能な情報伝送方法、記録方法及び記録媒体を提供することを目的とする。

【0 0 0 7】

また、本発明の他の目的は、暗号化された情報と暗号解除情報の同期のための情報を必要とすることなく、再生信号の暗号を正常に解読し得る情報伝送方法、記録方法及び記録媒体を提供することにある。

【0 0 0 8】

【課題を解決するための手段】

上記の目的を達成するため、本発明の情報伝送方法及び記録方法は、暗号化した所望の情報と、この所望の情報を誤り訂正する誤り訂正符号とを、再生側で正規のユーザに対してのみ暗号を解除して再生可能とするための、暗号解除情報と共に伝送あるいは記録する方法において、誤り訂正符号の完結周期内に、少なくとも一つの暗号解除情報を分散配置して伝送、若しくは暗号解除情報と共に同じ記録媒体に記録することを特徴とする。

【0 0 0 9】

この発明では、誤り訂正符号の完結周期と少なくとも一つの暗号解除情報の伝送あるいは記録周期とが同じであるため、誤り訂正符号による所望の情報の誤り訂正と、暗号解除情報による暗号解除とが同時に行えると共に、所望の情報と暗号解除情報との誤り確率を同一にできる。

【0 0 1 0】

また、本発明の記録方法は、上記の目的を達成するため、少なくとも映像情報を含む所望の情報と、この所望の情報の所定数の記録トラック又は記録セクタ周期で完結する所望の情報の誤り訂正符号とを暗号化して、デジタル信号形態で同じ記録媒体に記録する記録方法において、再生側で正規のユーザに対してのみ

暗号を解除して再生可能とするための暗号解除情報を、所定数の記録トラック又は記録セクタ周期内で分散配置して少なくとも一つ記録することを特徴とする。

【0011】

この発明では、誤り訂正符号の完結周期であるトラック数又はセクタ数と同じ数のトラック又はセクタに、少なくとも一つの暗号解除情報が記録されるため、記録媒体の再生側において誤り訂正符号による所望の情報の誤り訂正と、暗号解除情報による暗号解除とが同時に行えると共に、所望の情報と暗号解除情報との誤り確率を同一にできる。

【0012】

また、本発明の記録媒体は、上記の目的を達成するため、少なくとも映像情報が誤り訂正符号と共に暗号化されて固定長のデータブロック単位で予め定められたデータブロック数の各トラックに記録されているテープ状記録媒体であって、誤り訂正符号は複数トラックで完結するように記録されており、映像情報と誤り訂正符号の暗号化を正規の再生装置で解除するための暗号解除情報が、誤り訂正符号の完結トラックと同じトラック単位で完結するように分散配置されていることを特徴とする。

【0013】

この発明では、暗号化されている所望の情報と暗号解除情報とは、誤り訂正符号の同一の完結周期内で再生あるいは伝送できる。

【0014】

【発明の実施の形態】

次に、本発明の一実施の形態について図面と共に説明する。図1は本発明になる情報伝送方法及び記録方法の一実施の形態で、伝送、記録される暗号解除情報の信号中の配置説明図を示す。ここで、この実施の形態は、デジタル信号形態の映像情報及び音声情報を、磁気テープに回転ヘッドにより記録再生するデジタルVTRであるD-VHS（登録商標）を例にとって説明する。このD-VHSでは、磁気テープには所望のコンテンツ情報がデジタル信号の形態でテープ長手方向に対して傾斜した長手方向を持つデジタル信号記録トラックに記録される。

【0 0 1 5】

この磁気テープ上に形成されるデジタル信号記録トラックは、図2に示すように、シンクブロック（SB）と称される一定量のデータエリアを、回転ヘッドの走査に従って複数個配置することにより構成される。すなわち、デジタル信号記録トラックのトラックフォーマットは、図2に示す如く、2シンクブロックのマージン領域21、3シンクブロックのプリアンプル領域22、4シンクブロックのサブコード領域23、3シンクブロックのポストアンプル領域24、3シンクブロックのIBG領域25、1シンクブロックのプリアンプル領域26、336シンクブロックのメインコード領域（データ領域）27、2シンクブロックのポストアンプル領域28及びマージン領域29から構成されており、情報の記録領域として、メインコード領域27とサブコード領域23の2領域を有している。

【0 0 1 6】

なお、マージン領域29は回転ヘッドが取り付けられた回転体が、ドラムサーボにより30 r p s又は29.97 r p sで回転するように制御されるので、2シンクブロック又は2.356シンクブロックとされ、よって1トラック全体では356シンクブロック又は356.356シンクブロックで構成される。いずれの場合も、サブコード領域23は4シンクブロック、メインコード領域27は336シンクブロックで固定長に設定されている。メインコード領域27には、例えばMPEG (Moving Picture Experts Group) 2のトランスポートストリームの188バイトの各パッケージが隣接する2つのシンクブロックを単位として記録される。

【0 0 1 7】

上記の各シンクブロックのうち、メインコード領域27におけるシンクブロックのフォーマットは、図3に示すように、そのシンクブロック再生のための2バイトの同期信号（Sync）の領域31と、3バイトのアドレス情報（ID0、ID1、ID2）の領域32と、様々な情報を格納する2バイトのメインヘッダ格納領域33と、1バイトのデータ予備領域（DATA-AUX）34と、96バイトのデータ格納領域35と、このシンクブロックの情報の誤り訂正のための

8 バイトの内部パリティ格納領域 3 6 とが時系列的に合成された全部で 1 1 2 バイトの構成である。

【 0 0 1 8 】

データエリア 9 9 バイトのうち、後 9 6 バイトが情報のデータ格納領域 3 5 である。メインヘッダ格納領域 3 3 には、第 1 バイトの上位 4 ビットにフォーマット情報が、残りの下位 4 ビットと第 2 バイトの計 1 2 ビットにシンクブロック情報が割り当てられて記録されている。

【 0 0 1 9 】

領域 3 2 に記録される 3 バイトのアドレス情報 (I D 0、I D 1、I D 2) のうち、第 3 バイトのアドレス情報 I D 3 は第 1 バイトと第 2 バイトのアドレス情報 I D 0 と I D 1 のパリティである。また、アドレス情報 I D 0 は、図 4 に示すように、上位 4 ビットがシーケンスナンバー 4 1 を、ビット 3 からビット 1 までの 3 ビットがトラックペアナンバー 4 2 を示し、アドレス情報 I D 0 の最下位ビットとアドレス情報 I D 1 からなる計 9 ビットがシンクブロックナンバー 4 3 を示す。

【 0 0 2 0 】

上記のシーケンスナンバー 4 1 は、誤り訂正符号 (E C C) の繰り返し及び記録信号の周期を示すための番号で、ここでは、例えば 6 トラックで誤り訂正符号が完結するように記録されるものとする、シーケンスナンバー 4 1 は 6 トラック毎に値が増加していき、2 4 トラック周期で記録されるものとする、2 4 トラックで値が一巡する。

【 0 0 2 1 】

なお、6 トラックで誤り訂正符号が完結するように記録されるため、データと共に誤り訂正符号を構成するパリティ (外符号) は、1 8 0 シンクブロックでデータシャフリングが行われ、そのうちの 3 0 (= 1 8 0 シンクブロック / 6 トラック) シンクブロックずつが各トラックの、図 2 に示したメインコード領域 2 7 内に配置されて記録される。従って、メインコード領域 2 7 は 3 0 6 シンクブロックのデータ (デジタル映像信号など) と、3 0 シンクブロックのパリティ (外符号) とからなる。また、6 トラックで完結する誤り訂正符号は、2 0 1 6 (

= 336 × 6) シンクブロックからなる。

【0022】

また、図4に示すトラックペアナンバー42は、誤り訂正符号の完結ブロックを示すための番号で、この実施の形態が適用されるVTRではアジマス記録を行うために、第1のアジマス角のトラックと、第2のアジマス角のトラックとが交互に配置されるため、これら隣接する第1及び第2のアジマス角のトラックに同一番号がペアトラックナンバーとして割り当てられる。

【0023】

前述したように、ここでは誤り訂正符号が6トラックで完結するように記録されているので、上記のトラックペアナンバー42は、10進数で“0”、“1”、“2”を示す値がバイナリーコードで配置されて巡回的に繰り返される。なお、同一のトラックペアナンバーのそれぞれのトラックの識別は、アジマス角度が何かにより識別される。

【0024】

更に、シンクブロックナンバー43は、メインコード領域27内の336シンクブロックのうちの何番目のシンクブロックであるかを識別させるための番号である。

【0025】

さて、誤り訂正符号は、図3中のメインヘッダ領域33以後のすべてのデータに内符号（インナーコードで、内部パリティ36に相当）及び外符号（アウターコード）として適用されているが、6本のトラックにまたがって記録されるのは前述したように、メインコード領域27内に配置される誤り訂正符号である。

【0026】

そこで、この実施の形態では、上記の点に着目して、暗号解除情報を、この誤り訂正符号が完結する6トラック範囲に完結させてメインコード領域27内に記録することにより、メインコード領域27のデータの復号と同時に、暗号解除情報の復号ができ、しかも、メインコード領域27のデータと暗号解除情報の誤り確率を同一にできるので、効率的な記録再生ができるようにしたものである。なお、暗号解除情報には、バージョン情報や検査情報なども含む。

【0027】

次に、暗号解除情報の記録方法について更に詳細に説明する。メインコード領域 27 は、図 3 に示したフォーマットのシンクブロックが 336 個からなり、このシンクブロックを構成するデータ予備領域 34 に暗号解除情報が配置されて記録される。

【0028】

データ予備領域 34 は、図 1 に示すように、6 シンクブロック (SB) を一周期として記録され (つまり 6 バイト単位で記録され)、一周期内の 1 番目のデータ予備領域 34 にはパックヘッダ PC0 が記録され、残りの 2 番目から 6 番目の計 5 つのシンクブロックの各データ予備領域 34 にはパック情報 PC1 ~ PC5 が記録される。

【0029】

ここで、本実施の形態では、図 1 に示した PC0 ~ PC5 の計 6 バイトの 1 パックのうち、1 番目のパックヘッダ PC0 は、特別な情報であり、例えば、タイムコード、プログラムナンバー、テキストデータ、TOC 情報、暗号解除情報などの識別を行う。ここでは、PC0 のうち、1 バイトの値が (1111, 1xxx) で表される PC0 が、続く PC1 ~ PC5 に暗号解除情報が配置されていることを示すパックヘッダであり、xxx の部分がページ番号で、000 ~ 101 までの 6 ページ (6トラック) で一つの暗号化情報が記録される。

【0030】

すなわち、この実施の形態では、PC0 の値がそれぞれ (1111, 1000)、(1111, 1001)、(1111, 1010)、(1111, 1011)、(1111, 1100)、(1111, 1101) である、各トラックの 1 パックのパック情報 PC1 ~ PC5 による計 30 バイトで一つの暗号解除情報が分散記録されるので、他のパック情報に大きな影響を与えることがなく、また解読されにくいという効果もある。

【0031】

また、上記の 6 ページ (6トラック) は、誤り訂正符号の完結単位である、トラックペアナンバーが 0 ~ 3 である 6トラックであり、暗号解除情報は誤り訂正符

号の完結単位と同期して記録されるため、メインコード領域 27 のデータの復号と同時に、暗号解除情報の復号ができると共に、メインコード領域 27 のデータと暗号解除情報の誤り確率を同一にでき、また、処理の遅延時間を最小にできる。

【0032】

なお、上記の実施の形態では、D-VHS を例にとって説明したが、本発明はこれに限定されるものではなく、誤り訂正符号は 6トラック内に複数記録してもよく、また、他のデジタル信号記録再生装置にも適用できる。また、記録媒体は磁気テープに限定されるものではなく、光ディスクや磁気ディスクも適用可能であり、この場合は誤り訂正符号や暗号解除情報は、トラックに代えて所定のセクタ単位で完結するように記録する。

【0033】

更には、本発明は、記録再生装置ではなく、例えばパーソナルコンピュータ等の情報機器により図 2 及び図 3 のフォーマットの信号が伝送される場合に、図 1 に示したように暗号解除情報が伝送信号中に挿入されている伝送方式にも適用可能である。また、暗号解除情報は、隣り合う誤り訂正符号の完結単位で、同じでも異なってもよい。

【0034】

【発明の効果】

以上説明したように、本発明によれば、暗号解除情報が誤り訂正符号の完結周期内に分散して伝送あるいは記録されるため、暗号解除情報の解読を困難にでき、また、誤り訂正符号による所望の情報の誤り訂正と、暗号解除情報による暗号解除とが同時に行えるため、特にテープ状記録媒体に本発明を適用した場合は、テープの中途からでも短時間で再生情報を得ることができ、また、暗号化されている所望の情報と暗号解除情報との同期の問題を解決でき、同期できないときのデータの棄却を防止でき、また、その防止のための余分なメモリ等を不要にできる。

【0035】

また、本発明によれば、所望の情報と暗号解除情報との誤り確率を同一にできるため、効率の良い記録再生ができる。更に、本発明によれば、暗号化されてい

る所望の情報と暗号解除情報とは、誤り訂正符号の同一の完結周期内で記録あるいは伝送されるため、処理の遅延時間を最小にすることができ、再生応答の速い記録媒体を提供できる。

【図面の簡単な説明】

【図 1】

本発明方法により記録又は伝送される暗号化解除情報の一実施の形態の記録位置の説明図である。

【図 2】

本発明の記録トラックのフォーマットの一例を示す図である。

【図 3】

図 2 中のメインコード領域のデータブロックのフォーマットの一例を示す図である。

【図 4】

図 3 中のデータ予備領域の記録情報の一例を示す図である。

【符号の説明】

P C 0 パックヘッダ

P C 1 ～ P C 5 2 バイト目から 6 バイト目のパック情報

2 7 メインコード領域

3 2 アドレス情報領域

3 4 データ予備領域 (D a t a - A U X)

3 5 データ領域

3 6 内部パリティ

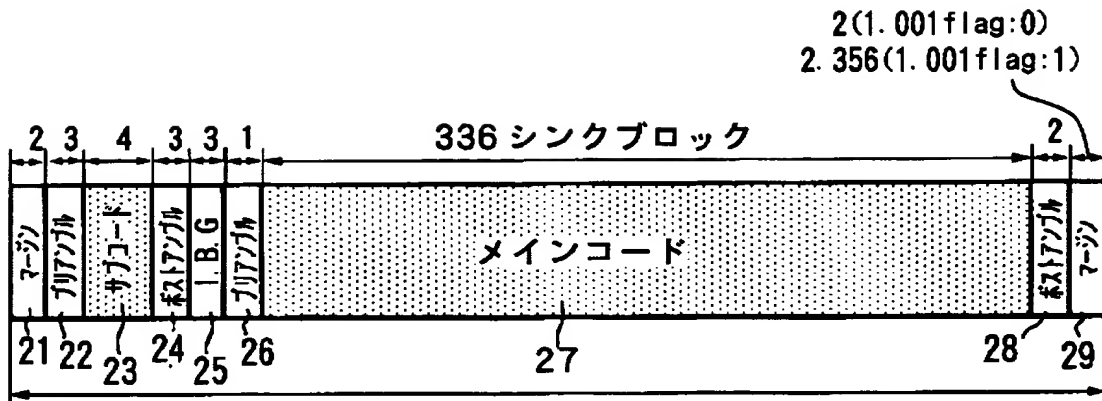
4 2 トラックペアナンバー

【書類名】 図面

【図 1】

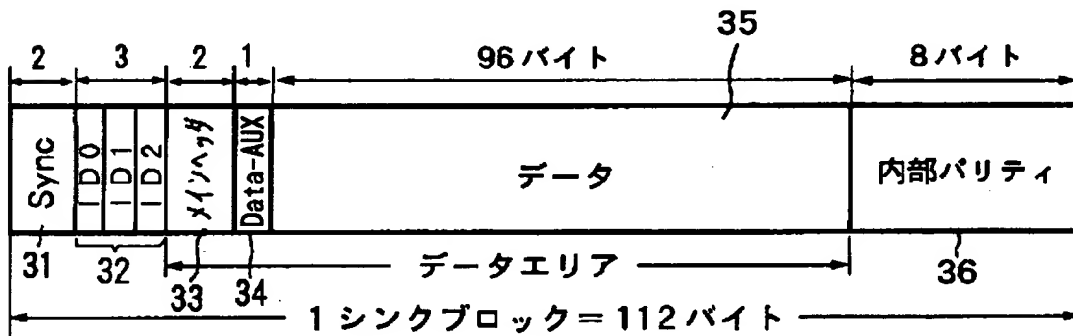
S B #	内 容
6 n	P C 0 (1111, 1xxx)
6 n + 1	P C 1
6 n + 2	P C 2
6 n + 3	P C 3
6 n + 4	P C 4
6 n + 5	P C 5

【図 2】

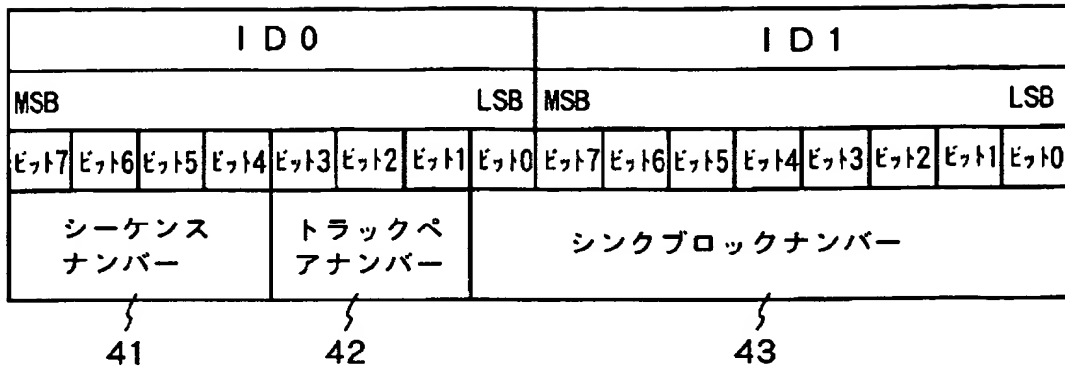


1トラック=356シンクブロック(1.001flag:0)
1トラック=356.356シンクブロック(1.001flag:1)

【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 暗号解除情報と映像情報とをディスクの異なる領域に記録して暗号を解除する方法を、磁気テープの記録再生装置に適用した場合は、暗号解除情報のアクセスに時間がかかり、テープ中途からの再生に支障をきたし、実用的でない。

【解決手段】 PC0～PC5の計6バイトの1パックのうち、1バイトの値が(1111, 1xxx)で表されるPC0が、続くPC1～PC5に暗号解除情報が配置されていることを示すパックヘッダであり、xxxの部分ページ番号で、000～101までの6ページ(6トラック)で一つの暗号化情報が記録される。各トラックの1パックのパック情報PC1～PC5による計30バイトで一つの暗号解除情報が分散記録されるので、他のパック情報に大きな影響を与えることがなく、また解読されにくいという効果もある。上記の6ページ(6トラック)は、誤り訂正符号の完結単位であり、暗号解除情報は誤り訂正符号の完結単位と同期して記録される。

【選択図】 図1

職権訂正履歴（職権訂正）

特許出願の番号	平成11年 特許願 第335502号
受付番号	59901152999
書類名	特許願
担当官	木村 勝美 8848
作成日	平成11年12月 1日

<訂正内容1>

訂正ドキュメント

書誌

訂正原因

職権による訂正

訂正メモ

【特許出願人】の【識別番号】を訂正しました。

訂正前内容

【特許出願人】

【識別番号】 000004392

【氏名又は名称】 日本ビクター株式会社

【代表者】 守随 武雄

訂正後内容

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【代表者】 守随 武雄

認定・付加情報

特許出願の番号	平成11年 特許願 第335502号
受付番号	59901152999
書類名	特許願
担当官	第八担当上席 0097
作成日	平成11年12月 8日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000004329
【住所又は居所】	神奈川県横浜市神奈川区守屋町3丁目12番地
【氏名又は名称】	日本ビクター株式会社

【代理人】

申請人	
【識別番号】	100085235
【住所又は居所】	東京都中央区日本橋人形町2丁目10番5号 T MA人形町ビル6階 松浦特許事務所
【氏名又は名称】	松浦 兼行

出 願 人 履 歴 情 報

識別番号 [000004329]

1. 変更年月日 1990年 8月 8日

[変更理由] 新規登録

住 所 神奈川県横浜市神奈川区守屋町3丁目12番地

氏 名 日本ビクター株式会社